02-21-03

GP/2131

EXPRESS MAIL CERTIFICATE

Date 2/19/03 Label No. EV 294035845US

I hereby certify that, on the date indicated above, this paper or fee was deposited with the U.S. Postal Service & that it was addressed for delivery to the Assistant Commissioner for Patents, Washington, DC 20231 by "Express Mail Post Office to Addressee" service.

L. Stantini L. Stantini

Name (Print) Signature

PLEASE CHARGE ANY DEFICIENCY UP TO $300.00 OR CREDIT ANY EXCESS IN THE FEES DUE WITH THIS DOCUMENT TO OUR DEPOSIT ACCOUNT NO. 04-0100

Customer No.: 07278

PATENT TRADEMARK OFFICE

Docket No.: 6727/0J351US0

DARBY & DARBY P.C.
Post Office Box 5257
New York, NY 10150-5257
212-527-7700

In re Application of: Itai DROR; Carmi David GRESSEL; Michael MOSTOVOY; Alexey MOLCHANOV

Serial No.: 09/854,853 Examiner : N/A

Confirmation No.: 8333

Filed: May 14, 2001 Art Unit: 2131

For: EXTENDING THE RANGE OF COMPUTATIONAL FIELDS OF INTEGERS

AMENDMENT TRANSMITTAL

Hon. Commissioner of
Patents and Trademarks
Washington, DC 20231

Sir:

Transmitted herewith is an amendment in the above-identified application. The fee has been calculated as shown below.

	Claims remaining after amendment	Highest number previously paid for		Present extra	Rate	Additional Fee
Total Claims	40	- 30	=	10	$18	$180.00
Independent	6	- 4	=	2	$84	$168.00
Multiple Dependent						$

Total additional fee for this amendment $348.00

[] Small Entity REDUCTION (Half of preceding total) $.00

[] No additional fee is required.

[X] A check in the amount of $348.00 is attached.

[**X**] Please charge any additional fees up to $500.00 or credit overpayment to Deposit Account No. 04-0100. A duplicate copy of this sheet is enclosed.

Respectfully submitted,

Dated: February 18, 2003

S. Peter Ludwig
Reg. No. 25,351
Attorney for Applicant(s)

DARBY & DARBY P.C.
Post Office Box 5257
New York, NY 10150-5257
212-527-7700

#10 / A

EXPRESS MAIL CERTIFICATE 2940358455US
Date 2/19/03 Label No. EV

I hereby certify that, on the date indicated above, this paper or fee was deposited with the U.S. Postal Service & that it was addressed for delivery to the Assistant Commissioner for Patents, Washington, DC 20231 by "Express Mail Post Office to Addressee" service.

L. Stantini A. Stantini
Name (Print) Signature

PLEASE CHARGE ANY DEFICIENCY UP TO $300.00 OR CREDIT ANY EXCESS IN THE FEES DUE WITH THIS DOCUMENT TO OUR DEPOSIT ACCOUNT NO. 04-0100

Customer No.:

Dkt. No. 6727/0J351

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of : DROR et al

Serial No. : 09/854,853 Group Art Unit: N/A

Filed : 14 May 2001 Examiner: N/A

For : EXTENDING THE RANGE OF COMPUTATIONAL FIELDS OF INTEGERS

Hon. Commissioner of
Patents and Trademarks
Washington, D.C. 20231

PRELIMINARY AMENDMENT

Sir:

Kindly amend the application as follows:

Kindly add the following new claims 31 - 40:

--31. A microelectronic apparatus for performing modular multiplication, squaring and reduction, the apparatus multiplying a multiplicand A by a multiplier B over a modulus N, wherein B is a serial fed radix 2^l multiplier comprising no more than k character multiplier

a1

segments, A comprises no more than k character multiplicand segments, and N has no more than k characters, each character having l bits, the apparatus comprising:

a first (B) register operative to store the multiplier B;

a modular multiplication device accepting multiplicands having no more than k characters, the modular multiplication device including a single accumulation device at least k characters long and operative to repeatedly receive a multiplicand and simultaneously output a character;

a digital logic sensing detector operative to anticipate that a non-zero character would be about to be output from the single accumulation device and to determine a number of times, Y_0, that the modulus N should be added into the single accumulation device so as to force the non-zero character to zero,

the modular multiplication device operative, during a first phase, to switch into the single accumulation device, in turn, multiplicand values, and to receive, character by character, the contents of the B register and the Y_0 value from the digital logic sensing detector, thereby to force up to k first output characters which are zero, the multiplicand values switched in turn into the accumulation device comprising less than 3 of the following three multiplicands: (a) an all-zero string value; (b) a portion of the multiplicand A; and (c) at least a portion of the modulus N; and

an output transfer mechanism, operative in a last phase

to unload at least a portion of a final modular multiplication result from the accumulation device.

32. Apparatus according to claim 31 for performing interleaved modular

multiplication and reduction in a plurality of interleaved iterations, wherein the Y_0 value used in the first phase is saved, and wherein said portion of the modulus N comprises a k-character least significant portion thereof,

the apparatus also comprising a second (S) register operative to store a temporary result S from an iteration i for use during a subsequent iteration i+1 and a third (N) register operative to store the modulus N, wherein n, the number of characters in the third (N) register, is larger than k;

the modular multiplication device being operative, in a first phase, to multiply a plurality of slices of A during the plurality of interleaved iterations respectively, by B,

the modular multiplication device being operative, during a second phase between the first and last phases, to switch into the single accumulation device, in turn, multiplicand values, and to receive multiplier values from the B and N registers, the multiplicand values switched in turn into the accumulation device comprising less than 3 of the following three multiplicands: (a) an all-zero string value; (b) a portion of the multiplicand A; and (c) the Y_0 value as saved from the first phase;

the apparatus also comprising a serial addition device operative, during each iteration, to summate the temporary result value S in the second (S) register with the character output by the accumulation device, thereby to generate n-k least significant characters of a new temporary result, which characters are stored in the second (S) register, for the next in turn iteration.

33. Apparatus according to claim 31 wherein all addition, accumulation and multiplication operations are switchable to be performed either with carries or without carries, over GF(p) or over $GF(2^q)$.

34. Apparatus according to claim 31 which employs Y_0 as the next character of a polynomial based modular reducing quotient deterministically.

35. An apparatus as in claim 31 wherein the digital logic sensing detector is operative to receive the following four inputs:

i. the product of the least significant character in the A register multiplied by a current value from the B register, in modulus 2^l;

ii. the first emitted carry out character from the accumulation device;

iii. the contents of the second from the right character in the accumulation device;

iv. the negative multiplicative inverse of the right-hand character in the N register.

36. An apparatus as in claim 32 wherein the digital logic sensing detector is operative to receive the following six inputs:

i. the product of the least significant character in the A register multiplied by a current value from the B register, in modulus 2^l;

ii. the first emitted carry out character from the accumulation device;

iii. the contents of the second from the right character in the accumulation device;

iv. the negative multiplicative inverse of the right-hand character in the N register.

v. the next in turn character in the S register; and

vi. the carry out character from the serial addition device.

37. A method for performing modular multiplication, squaring and reduction, including multiplying a multiplicand A by a multiplier B over a modulus N, wherein B is a serial fed radix 2^l multiplier comprising no more than k character multiplier segments, A comprises no more than k character multiplicand segments, and N has no more than k characters, each character having l bits, the method comprising:

storing a multiplier B in a first (B) register;

providing a modular multiplication device accepting multiplicands having no more than k characters, the modular multiplication device including a single accumulation device at least k characters long and operative to repeatedly receive a multiplicand and simultaneously output a character;

a1

anticipating that a non-zero character would be about to be output from the single accumulation device and determining a number of times, Y_0, that the modulus N should be added into the single accumulation device so as to force the non-zero character to zero,

during a first phase, switching into the single accumulation device, in turn, multiplicand values, and receiving, character by character, the contents of the B register and the Y_0 value from the digital logic sensing detector, thereby to force up to k first output characters which are zero, the multiplicand values switched in turn into the accumulation device comprising less than 3 of the following three multiplicands: (a) an all-zero string value; (b) a portion of the multiplicand A; and (c) at least a portion of the modulus N; and

in a last phase, unloading a final modular multiplication result from the accumulation device.

38. A method according to claim 37 for performing interleaved modular

multiplication and reduction in a plurality of interleaved iterations, wherein the Y_0 value used in the first phase is saved, and wherein said portion of the modulus N comprises a k-character least significant portion thereof, the method also comprising:

providing a second (S) register operative to store a temporary result S from an iteration i for use during a subsequent iteration i+1 and a third (N) register operative to store the modulus N, wherein n, the number of characters in the third (N) register, is larger than k;

the modular multiplication device being operative, in the first phase, to multiply a plurality of slices of A during the plurality of interleaved iterations respectively, by B,

the modular multiplication device being operative, during a second phase between the first and last phases, to switch into the single accumulation device, in turn, multiplicand values, and to receive multiplier values from the B and N registers, the multiplicand values switched in turn into the accumulation device comprising less than 3 of the following three multiplicands: (a) an all-zero string value; (b) a portion of the multiplicand A; and (c) the Y_0 value as saved from the first phase,

the method also comprising summating, during each iteration, the temporary result value S in the second (S) register with the character output by the accumulation device, thereby to generate a new temporary result, for the next in turn iteration.

39. A method according to claim 37 wherein all addition, accumulation and multiplication operations are switchable to be performed either with carries or without carries, over GF(p) or over $GF(2^q)$.

40. A method according to claim 37 which deterministically employs Y_0 as the next character of a polynomial based modular reducing quotient.--